

## Amendments to the Claims

1. (Currently Amended) A method for determining if an item is a fraudulent item, the method comprising the steps of:

obtaining by radio means a first number from an RFID tag associated with the item or item's packaging;

~~determining electronically reading a second number that is printed on the item or item's packaging of the item and is a public-key signature of the first number;~~

utilizing a public-key cryptographic process and ~~the first number~~ contents of the RFID tag to cryptographically ~~verify~~ decide whether the second number is a public-key signature of the first number; and

determining ~~the product's authenticity of the item~~ based on the ~~verification~~ result of the decision.

2-4. (Cancelled)

5. (Currently Amended) The method of claim 1 wherein the step of determining the ~~products~~ item's authenticity comprises ~~the step of associating the product-item with an authentic product item~~ if the signature is verified, otherwise associating the ~~product-item~~ with a forged ~~productitem~~.

6. (Currently Amended) A method of manufacturing a product in order to prevent forgery, the method comprising the steps of:

~~obtaining an anti-forgery RFID tag of a type that is pre-programmed with an unalterable first number, wherein the unalterable first number is rarely the same number as unalterable first numbers in other anti-forgery RFID tags of the same type;~~

programming an anti-forgery RFID tag, pre-programmed with an unalterable first number, with a second number into the anti-forgery RFID tag, the unalterable first number probabilistically rarely the same number as unalterable first numbers in other anti-forgery RFID tags;

determining a third number that is a cryptographic signature over the first and second numbers;

affixing the anti-forgery RFID tag comprising the first and second numbers to either the product or the packaging associated with the product; and

affixing the third number to either the product or the packaging associated with the product.

7. (Cancelled)

8. (Previously Presented) The method of claim 6 wherein the step of affixing the third number to either the product or the packaging associated with the product comprises the step of printing the third number on the product or the product's packaging.

9-10. (Cancelled)

11. (Currently Amended) A method comprising the steps of:

obtaining an RFID tag comprising a first number;

utilizing a private key and the first number to create a second number that is a cryptographic signature, such that cryptographic verification of the second number insures a product's authenticity of an item; and

affixing the second number and the RFID tag to the item or the item's packaging.

12-18. (Cancelled)

19. (Previously Presented) The method according to claim 1 wherein a bar code is used for rendering the second number that is printed on the item or item's packaging.

20. (Previously Presented) The method according to claim 11, wherein a bar code is used for rendering the second number that is affixed on the item or item's packaging.

21. (Currently Amended) A method for determining if an item is a fraudulent item, the method comprising the steps of:

obtaining by radio means a first and second number from an RFID tag, wherein the first number is unalterable and unique or semi-unique and the second number is associated with the item;

electronically reading a third number that is a public-key signature over the first and second numbers;

utilizing a public-key cryptographic process and the first and second numbers to cryptographically decide whether verify the third number is a public-key signature of a combination of the first and second numbers; and

determining the product's authenticity of the item based on the result of the decision verification.

22. (Currently Amended) The method according to claim 21 further comprising the step of: verifying that electronically determining whether the RFID is an anti-forgery RFID tag.

23. (Currently Amended) The method according to claim ~~22~~21, wherein the verification comprises verifying one of further comprising electronically determining whether a specific physical feature and/or a behavioral feature matches that of the an anti-forgery RFID tag. {page 6, lines 1-8}

24. (Currently Amended) The method according to claim 21 further comprising the step of: verifying that the second number is associated with the item.

25. (Currently Amended) The method according to claim 24, wherein the verification is performed visually electronically using an optical scanner.

26. (Currently Amended) The method according to claim 21 further comprising the step of: verifying that electronically determining whether the second number is an Electronic Product Code (EPC) of the item.

27. (Previously Presented) The method according to claim 21, wherein the reading is performed by a bar code scanner.

28. (Previously Presented) A method according to claim 6, wherein the second number is associated with the product.

29. (New) A method according to claim 1, wherein:

- a third number is obtained from the RFID tag when the first number is obtained,
- the third number is concatenated with, but a separate number than, the first number,
- the third number includes product information of the item,
- the public-key cryptographic process is used with the first and third numbers, and
- only if the public-key cryptographic process cryptographically decides that the second number is a public-key signature of the first and third numbers is the product determined to be authentic.

30. (New) A method according to claim 29, wherein the first number does not contain product information of the item.

31. (New) A method according to claim 6, wherein the first number does not contain product information of the item and the second number contains product information of the item.

32. (New) A method according to claim 11, wherein the first number does not contain product information of the item.

33. (New) A method according to claim 21, wherein the first number does not contain product information of the item.